UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/578,113	01/08/2007	Ae-Soon Park	1403-03 PCT US	5006

66547 7590 10/12/2010

THE FARRELL LAW FIRM, LLP
290 Broadhollow Road
Suite 210E
Melville, NY 11747

EXAMINER	
HWANG, STAMFORD	
ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
10/12/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/578,113	PARK ET AL.	
	Examiner	Art Unit	
	STAMFORD HWANG	2617	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 September 2010*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-47* is/are pending in the application.

4a) Of the above claim(s) *1-24* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *25-47* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 May 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

Applicant's arguments with respect to Claims 25, 33, 39 and 44 have been considered but are moot in view of the new ground(s) of rejection.

Claim Objections

Claim 25 is objected to because of the following informalities: Claim 25 recites "at least one authentication mode than can be supported" and the limitation should read "at least one authentication mode that can be supported". Appropriate correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claim 25 - 27, 30, 31, 33 - 36 and 39 - 47 are rejected under 35 U.S.C. 102(e) as being anticipated by Barriga-Caceres et al. (U.S. 2003/0163733 A1).

With respect to Claim 25, Barriga-Caceres et al. teaches a method comprising:

- transmitting a subscriber station basic capability negotiation request (SBC-REQ) message to the base station, the SBC-REQ message including information on at least one authentication mode than can be supported by the subscriber station **(Fig. 5B, step C-503 and Paragraph [0101]; Step C-503 transmits the authentication mode selected by user, among different authentication mechanisms available for the user.)**;
- receiving a subscriber station basic capability negotiation response (SBC-RSP) message including information on an authentication mode that is selected by the base station among the at least one authentication mode **(Fig. 5B, step C-504 and Paragraph [0101]; As the user chooses to authenticate via the SIM card, as shown as an example in Paragraph [0101], the base station then invokes the chosen authentication by inquiring the related credentials with step C-504. Further, as the user provides information regarding only one authentication mode, the base station picks that only one authentication mode to proceed.)**; and
- transmitting an authentication request message corresponding to the selected authentication mode to the base station **(Fig. 5B, step C-505 and Paragraph [0101])**.

With respect to Claim 26, Barriga-Caceres et al. further teaches wherein each of the SBC-REQ message and the SBC-RSP message includes a parameter for selecting the authentication mode **(Paragraph [0101]; IMSI is the parameter)**.

With respect to Claim 27, Barriga-Caceres et al. further teaches wherein the selected authentication mode includes at least one of a digital certificate based authentication mode and an extensible authentication protocol (EAP) based authentication mode **(Paragraph [0101]; "Provided that a SIM-based authentication had been selected, the IMSI is used as applicable identity and is encapsulated in an Attribute Value Pair (AVP) of an Extensible Authentication Protocol (EAP) and in the User-Name AVP")**.

With respect to Claim 30, Barriga-Caceres et al. further teaches wherein, when the selected authentication mode is an EAP-based authentication mode, the authentication request message is a message for requesting the authentication by an authentication, authorization, and accounting (AAA) server, wherein the AAA server is connected to the base station and performs the authentication **(Fig. 5B, AAA 44 and Paragraph [0101])**.

With respect to Claim 31, Barriga-Caceres et al. further teaches wherein, when the selected authentication mode is an EAP-based authentication mode, the authentication request message includes an EAP payload, wherein the EAP payload includes data for the authentication **(Paragraphs [0101] and [0102])**.

With respect to Claim 33, Barriga-Caceres et al. teaches a method comprising:

- receiving a subscriber station basic capability negotiation request (SBC-REQ) message from the subscriber station mode, the SBC-REQ message including information on at least one authentication mode that can be supported by the subscriber station **(Fig. 5B, step C-503 and Paragraph [0101]; Step C-503 transmits the authentication mode selected by user, among different authentication mechanisms available for the user.)**;
- selecting an authentication mode from among the at least one authentication mode **(Fig. 5B, step C-504 and Paragraph [0101]; As the user chooses to authenticate via the SIM card, as shown as an example in Paragraph [0101], the base station then invokes the chosen authentication by inquiring the related credentials with step C-504. Further, as the user provides information regarding only one authentication mode, the base station picks that only one authentication mode to proceed.)**;
- transmitting a first response message to the subscriber station, the first response message including information on the selected authentication mode **(Fig. 5B, step C-504 and Paragraph [0101])**;
- receiving an authentication request message corresponding to the selected authentication mode from the subscriber station **(Fig. 5B, step C-505 and Paragraph [0101])**; and

- transmitting a second response message to the subscriber station, the second response message representing a result of the authentication performed in accordance with the authentication request message **(Fig. 5B, step C-513, Fig. 5C, steps C-25 or C-29)**.

With respect to Claim 34, Barriga-Caceres et al. further teaches wherein the authentication mode includes at least one of a digital certificate based authentication mode and an extensible authentication protocol (EAP) based authentication mode **(Paragraph [0101]; "Provided that a SIM-based authentication had been selected, the IMSI is used as applicable identity and is encapsulated in an Attribute Value Pair (AVP) of an Extensible Authentication Protocol (EAP) and in the User-Name AVP")**.

With respect to Claim 35, Barriga-Caceres et al. further teaches wherein, when the selected authentication mode is an EAP-based authentication mode, the receiving of the authentication request message comprises requesting an authentication, authorization, and accounting (AAA) server to perform an authentication through an standardized authentication protocol of an upper layer **(Fig. 5B, AAA 44 and Paragraph [0101])**.

With respect to Claim 36, Barriga-Caceres et al. further teaches wherein, when the selected authentication mode is an EAP-based authentication mode, the second

response message includes an EAP payload, wherein the EAP payload includes data for the authentication **(Paragraphs [0101] and [0102])**.

With respect to Claim 39, Barriga-Caceres et al. teaches an apparatus comprising:

- message parser configured to receive a first message from the subscriber station, the first message including information on at least one authentication mode that can be supported by the subscriber station **(Fig. 5B, step C-503 and Paragraph [0101]; Step C-503 transmits the authentication mode selected by user, among different authentication mechanisms available for the user.)**;
- an authentication controller configured to select an authentication mode that can be performed by the base station among the at least one authentication mode, and for transmitting a second message including information on the selected authentication mode to the subscriber station **(Fig. 5B, step C-504 and Paragraph [0101]; As the user chooses to authenticate via the SIM card, as shown as an example in Paragraph [0101], the base station then invokes the chosen authentication by inquiring the related credentials with step C-504. Further, as the user provides information regarding only one authentication mode, the base station picks that only one authentication mode to proceed.)**;

- wherein the message parser is further configured to receive an authentication request from the subscriber station by receiving a privacy key management request (PKM-REQ) message having a message type according to the selected authentication mode **(Fig. 5B, step C-505 and Paragraph [0101])**; and
- wherein the authentication reply message generator is further configured to transmit a privacy key management response (PKM-RSP) message having a message type according to the selected authentication mode to the subscriber station in response to the authentication request **(Fig. 5B, step C-513, Fig. 5C, steps C-25 or C-29)**.

With respect to Claim 40, Barriga-Caceres et al. further teaches wherein, when the selected authentication mode is an extensible authentication protocol (EAP) based authentication mode, the message type of each of the PKM-REQ message and the PKM-RSP message is an EAP transfer including an EAP payload, wherein the EAP payload includes data for the authentication **(Paragraphs [0101] and [0102])**.

With respect to Claim 41, Barriga-Caceres et al. teaches a method comprising:

- receiving a subscriber station basic capability negotiation request (SBC-REQ) message from the subscriber station, the SBC-REQ message including a parameter representing at least one authentication mode that

can be supported by the subscriber station **(Fig. 5B, step C-503 and Paragraph [0101]; IMSI is the parameter)**;

- selecting an authentication mode that can be performed by the base station among the at least one authentication mode **(Fig. 5B, step C-504 and Paragraph [0101])**; and
- transmitting a subscriber station basic capability negotiation response (SBC-RSP) message to the subscriber station, the SBC-RSP including a parameter representing the selected authentication mode **(Fig. 5B, step C-504 and Paragraph [0101])**.

.

With respect to Claim 42, Barriga-Caceres et al. teaches further comprising:

- receiving a privacy key management request (PKM-REQ) message having a message type according to the selected authentication mode **(Fig. 5B, step C-505 and Paragraph [0101])**; and
- transmitting a privacy key management response (PKM-RSP) message having a message type according to the selected authentication mode to the subscriber station in response to the PKM-REQ message **(Fig. 5B, step C-513, Fig. 5C, steps C-25 or C-29)**.

With respect to Claim 43, Barriga-Caceres et al. further teaches wherein, when the selected authentication mode is an extensible authentication protocol (EAP) based authentication mode, the message type of each of the PKM-REQ message and the

PKM-RSP message is an EAP transfer including an EAP payload, wherein the EAP payload includes data for the authentication **(Paragraphs [0101] and [0102])**.

With respect to Claim 44, Barriga-Caceres et al. teaches a method comprising:

- setting an extensible authentication protocol (EAP) based authentication mode as an authentication mode by negotiating with the subscriber station, wherein the EAP based authentication mode is selected by the base station from among at least one authentication mode that can be supported by the subscriber station **(Fig. 5B, steps C-503, C-504 and Paragraph [0101]; Step C-503 transmits the authentication mode selected by user, among different authentication mechanisms available for the user. As the user chooses to authenticate via the SIM card, as shown as an example in Paragraph [0101], the base station then invokes the chosen authentication by inquiring the related credentials with step C-504. Further, as the user provides information regarding only one authentication mode, the base station picks that only one authentication mode to proceed.)**;
- receiving an authentication request by receiving a privacy key management request (PKM-REQ) message from the subscriber station, the PKM-REQ message having a message type according to the EAP-based authentication mode **(Fig. 5B, step C-505 and Paragraph [0101])**; and

- transmitting a privacy key management response (PK_M-RSP) message to the subscriber station in response to the authentication request, the PKM-RSP message having a message type according to the EAP based authentication mode **(Fig. 5B, step C-513, Fig. 5C, steps C-25 or C-29)**.

With respect to Claim 45, Barriga-Caceres et al. further teaches wherein the message type of each of the PKM-REQ message and the PKM-RSP message is an EAP transfer including an EAP payload, and the EAP payload includes data for the authentication **(Paragraphs [0101] and [0102])**.

With respect to Claim 46, Barriga-Caceres et al. teaches an apparatus comprising:

- an authentication request message generator configured to transmit a first message to the base station, the first message including information on at least one authentication mode that can be supported by the subscriber station **(Fig. 5B, step C-503 and Paragraph [0101]; Step C-503 transmits the authentication mode selected by user, among different authentication mechanisms available for the user.)**; and
- an authentication reply message parser configured to receive a second message from the base station, the second message including information on an authentication mode selected by the base station among the at least one authentication mode **(Fig. 5B, step C-504 and Paragraph [0101]; As**

the user chooses to authenticate via the SIM card, as shown as an example in Paragraph [0101], the base station then invokes the chosen authentication by inquiring the related credentials with step C-504. Further, as the user provides information regarding only one authentication mode, the base station picks that only one authentication mode to proceed.);

- wherein the authentication request message generator is further configured to receive an authentication by transmitting a privacy key management request (PKM-REQ) message to the base station, the PKM-REQ message having a message type according to the selected authentication mode **(Fig. 5B, step C-505 and Paragraph [0101])**; and
- wherein the authentication reply message parser is further configured to receive a privacy key management response (PKM-RSP) message having a message type according to the selected authentication mode from the base station in response to the authentication request **(Fig. 5B, step C-513, Fig. 5C, steps C-25 or C-29)**.

With respect to Claim 47, Barriga-Caceres et al. further teaches wherein, when the selected authentication mode is an extensible authentication protocol (EAP) based authentication mode, the message type of each of the PKM-REQ message and the PKM-RSP message is an EAP transfer including an EAP payload, and wherein the EAP payload includes data for the authentication **(Paragraphs [0101] and [0102])**.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 28, 29, 32, 37 and 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barriga-Caceres et al. (U.S. 2003/0163733 A1) as applied to Claims 25 and 33 above, and further in view of Aura (U.S. 7,272,381 B2).

With respect to Claim 28, Barriga-Caceres et al. teaches all of the limitations in Claim 25 as discussed above. Barriga-Caceres et al. further teaches the authentication request message is a message for requesting the authentication by the base station **(Fig. 5B, step C-505 and Paragraph [0101])**.

Barriga-Caceres et al. does not explicitly teach "when the selected authentication mode is a digital certificate based authentication mode, the authentication request message is a message for requesting the authentication by the base station."

Aura teaches the use of various global identifiers, including home IP, MAC address or GSM IMSI, to identify misuse of the mobile access network and to function as a trust parameter for secure transmission **(Col. 13, lines 38 - 67)**.

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the method in Barriga-Caceres et al. to include digital identifiers, as taught by Aura, to secure the transmission between two nodes.

With respect to Claim 29, Barriga-Caceres et al. teaches all of the limitations in Claim 25 as discussed above. Barriga-Caceres et al. further teaches the authentication request message includes an authentication information message and an authorization request message **(Fig. 5B, step C-505 and Paragraph [0101])**.

Barriga-Caceres et al. does not explicitly teach "when the selected authentication mode is a digital certificate based authentication mode, the authentication request message includes an authentication information message and an authorization request message."

Aura teaches the use of various global identifiers, including home IP, MAC address or GSM IMSI, to identify misuse of the mobile access network and to function as a trust parameter for secure transmission **(Col. 13, lines 38 - 67)**.

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the method in Barriga-Caceres et al. to include digital identifiers, as taught by Aura, to secure the transmission between two nodes.

With respect to Claim 32, Barriga-Caceres et al. teaches all of the limitations in Claim 25 as discussed above. Barriga-Caceres et al. further teaches wherein the authentication request message is a privacy key management request (PKM-REQ) message **(Fig. 5B, step C-505 and Paragraph [0101])**.

Barriga-Caceres et al. does not explicitly teach "wherein the authentication request message is a privacy key management request (PKM-REQ) message included in a medium access control (MAC) message."

Aura teaches the use of various global identifiers, including home IP, MAC address or GSM IMSI, to identify misuse of the mobile access network and to function as a trust parameter for secure transmission **(Col. 13, lines 38 - 67)**.

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the method in Barriga-Caceres et al. to include digital identifiers, as taught by Aura, to secure the transmission between two nodes.

With respect to Claim 37, Barriga-Caceres et al. teaches all of the limitations in Claim 33 as discussed above. Barriga-Caceres et al. further teaches the second response message includes an authentication reply message **(Fig. 5B, step C-513, Fig. 5C, steps C-25 or C-29)**.

Barriga-Caceres et al. does not explicitly teach "when the selected authentication mode is a digital certificate based authentication mode, the second response message includes an authentication reply message."

Aura teaches the use of various global identifiers, including home IP, MAC address or GSM IMSI, to identify misuse of the mobile access network and to function as a trust parameter for secure transmission **(Col. 13, lines 38 - 67)**.

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the method in Barriga-Caceres et al. to include digital identifiers, as taught by Aura, to secure the transmission between two nodes.

With respect to Claim 38, Barriga-Caceres et al. teaches all of the limitations in Claim 33 as discussed above. Barriga-Caceres et al. further teaches wherein the second response message is a privacy key management response (PKM-RSP) message **(Fig. 5B, step C-505 and Paragraph [0101])**.

Barriga-Caceres et al. does not explicitly teach "wherein the second response message is a privacy key management response (PKM-RSP) message included in a medium access control (MAC) message."

Aura teaches the use of various global identifiers, including home IP, MAC address or GSM IMSI, to identify misuse of the mobile access network and to function as a trust parameter for secure transmission **(Col. 13, lines 38 - 67)**.

It would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the method in Barriga-Caceres et al. to include digital identifiers, as taught by Aura, to secure the transmission between two nodes.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to STAMFORD HWANG whose telephone number is (571)270-5578. The examiner can normally be reached on Monday ~ Friday 9:00AM ET~ 6:00PM ET.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Charles Appiah can be reached on (571)272-7904. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S.H./

/Charles N. Appiah/
Supervisory Patent Examiner, Art Unit 2617